

WHAT IS CLAIMED IS:

1. A digital signing method comprising steps of:
generating shares of a private signature key;
storing shares in separate electronic signing devices;
certifying multiple authorizing agents for signing devices; and
for each of a plurality of signing devices, affixing a partial signature to an electronic message in response to authorization from a minimum number of authorizing agents;
wherein a plurality of partial signatures constitutes a digital signature.
2. A system for affixing digital signatures to electronic documents comprising:
a plurality of intercommunicative signing devices, each signing device comprising an electronic device programmed to receive an electronic document and to affix a partial signature using a signature key share in response to a predetermined number of authorizations; and
a plurality of authorizing agents, each agent communicative with an associated signing device, each agent comprising an electronic device programmed to provide an authorization to an associated signing device.
3. A system of interlocked rings of signing devices for affixing digital signatures to electronic documents comprising:

a first set of signing devices, said first set comprising a plurality of electronic devices, each device programmed to receive an electronic document and affix a partial signature for a first signature key, a plurality of said partial signatures comprising a first digital signature;

a second set of signing devices, said second set comprising a plurality of electronic devices, each device programmed to receive an electronic document and affix a partial signature for a second signature key, a plurality of said partial signatures comprising a second digital signature;

wherein said first includes at least one member which is not in said second set, and said first and second sets include at least one common member.

4. An electronic method for delegated use of an electronic key comprising steps of:

storing said key in a first electronic device;

communicating an electronic delegation certificate to a delegate;

sending a request and the delegation certificate from the delegate to the first electronic device; and

using said first electronic device to use the electronic key in response to the request and the delegation certificate.